Human Computer Interaction and Security (HCI-Sec)

Iqra Khalil[1], Kanwal Zahoor[2], Saima Amber[3]

Abstract---The rapid proliferation of internet and technologies create many security related issues in business and local environment. Although the growing use rate shows that, there is a demand and need, to develop applications therefore a secure web infrastructure is also required. It is shown that privacy issues are not taken seriously by users. To provide a secure environment to the users, HCI studies and theories help to developers as HCI is highly concerned about trust of user with their proprietary information as well as enhance system's quality. This paper is about to identify user's concern about HCI-Sec in applications to ensure their personal information and highlight usability of security features in systems.

Key Words: Privacy, Human computer interaction, Information Security, Interactive.

1. INTRODUCTION

Privacy is developing as an important element for interactive systems. Many applications exists which offers some security tasks. This is necessary in all those applications that are working over internet and involves security threats. An application must be secure enough to provide protection from these security threats. But for the user must have all the knowledge about the system/application. The HCI design-user interface need to be address in different ways like application should be smart enough that people may understand how to secure their information. Some users are not experienced enough and are not able to change setting according to their need so they are forced to use default setting. The are not aware of how to change security settings as the designer has not kept in mind all the HCI principles.[1] In this paper an attempt has been made to provide easier way to use security feature in applications and the aim is to provide security overview in human computer interaction, concentrating on issues related to the design and evaluation of end-user system that have security allegations.

2. BACKGROUND

In order to inspect and evaluate the principle of HCI only computer related information is not enough. Many other skills are required. A developer must design a suitable user interface where learnability and efficiency will be high. The extreme objective of HCI is to advance the communication between human and computer. It may be attained by designing applications that all the features must be used by users. The usability of system decreases when security measures have to be taken serious like, Password must be used to access valid access. The password is more complex and longer, can be alphanumeric, and then system is safer.[2] So, if guides are produced that improve the HCI-Sec aspects of an application, it may be easier to use security options. The stability of HCI-Sec is to make the system stronger, more reliable and more reliable.

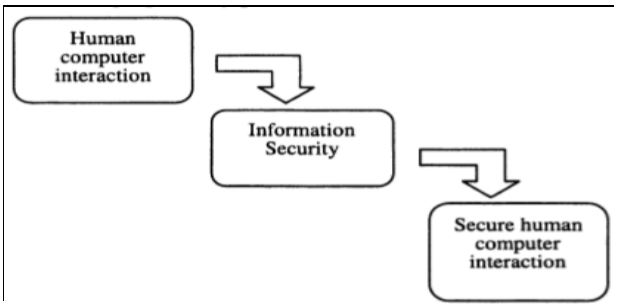

Figure 1. Human Computer Interaction Influence

Secure human computer interaction is most needed feature for e-commerce environments. Users want to assure that the interface by which they enter their credit card information for transaction will be protected against unauthorized modification.

3. HUMAN COMPUTER INTERACTION

A good user interface may benefit in many ways as it increases productivity and reduces errors. Well-

designed interfaces allow user to perform well. The three main modules in HCI are personal, computers and their relation (interaction). All modules are described concisely.

• Human – The user who uses the system.
• Computer – Hardware on which software is working.
• Interaction –The way in which user interact, uses or communicate with the system.

The main human resources that are used through HCI includes Perception –Gaining knowledge using senses, Cognition– The process of understating the processing of Information and Physiology. Perception is font category and size, color contrast etc. The reasoning resource, communications displayed should be definite with strong response choices for the user.[6]

4. INFORMATION SECURITY

IS is discussed in five services that are integrity, non-repudiation, authorization, confidentiality, identification & authentication. These services are necessary to guarantee that data is ensured and secured. Identification & authentication is the initial move towards implementing security. Authorization is the next stage is to decide whether the confirmed matter has the privilege to get to the computer facilities being referred to. All material must be severely available to authorized users only. Confidentiality is that only authorized parties will be able to access information. Confidentiality is necessary but integrity should be guaranteed too. So only the authorized user will be able to change the content. Non-repudiation is that no act of changing content can damage information security. These services must be accessible, visible, and functional from the perspective of human computer interaction to obtain information security.

5. HCI FOR INFORMATION SECURITY TECHNOLOGY

People are responsible for security issues which results in computer systems failure. It is possible to advance or enhance the execution of information security by means of consideration to some aspects. First of all understand the problem which occurs while providing secure interaction. Next complexity reduces security. Information security is only provided when all the features are visible to user and he knows how to use it.[2]

6. HCI-S GUIDELINES

Here are some HCI rules that presentation should follow to have correct HCI features. Ten important guidelines were formed and applications were estimated against for each one of them.

Perceptible organization state and safety purposes: All the security related function must be visible to the user he should not have to search them in order to apply changes. The system should always keep clients educated about what is happening, through suitable feedback within sensible time[4]. Much of the time, the display of the present security state can be utilized to give clients reflexive feedback of data security. Visibility of the system security state contributes to the working of trust and is therefore one standard for effective human-machine connection in security applications. Security must be visible without being nosy, as clients would prefer documents, dynamic symbols when security capacities are being executed on a system.

A. Security should be easily used: Interface should be designed in a way that it requires less effort to use of security features. The interface ought to be carefully compose and require negligible exertion so as to make utilization of security highlights. Moreover the security settings ought not to be set in a few distinct areas inside the application, since it will be hard for the client to find every last one of them.

B. Suitable for advanced as well as first time users: Applications are developed for use of both new and experienced users. So show enough information for an experienced user and detailed information for new user. There must be both shortcuts as well as defined methods for any function in application so that new user uses well defined methods to perform the work and experienced user may use shortcuts. Application may be simple and shortcut must be available for advanced users.

C. Avoid heavy use of technical vocabulary or advanced terms: Many people who uses applications may not have good vocabulary or language skills. If the designer uses feature containing difficult vocabulary user will definitely get confused in selecting the appropriate function according to his need, so use easy words and vocabulary in order to avoid misunderstandings.

D. Handle errors appropriately: Good error messages are suspicious interaction design which avoids a problem from happening in the first place. Therefore, system should not contain error-prone elements and should forestall possible user errors. Errors produced by the use of security feature could be prohibited and minimized.

E. Allow customization without risk to be trapped: New as well as old users are sometime not aware of proper functionality of some features. Exit path must be available if any function are chosen by mistake because in case if user experience wrong selection and no immediate exit he will never use any security feature until he is not properly aware of it. Need of exit path is necessary.
Example: in many application there is back button or if we press esc button on keyboard we are out of that particular area.

F. Easy to setup security settings: Security setting are basic need of user. To implement security as needed by clients all the settings available must be easy to understand, visible and vocabulary should be easily understandable. It should be easy so that anyone can change settings according to their needs.

G. Suitable Help and documentation for the available security: Help and documentation must be provided for new users. Provide clients quick access to help resources. Organize help around their tasks and goals. Make complete and accurate help. Write all appropriate thing in the documents.

H. Make the user feel protected: Guarantee the users that his work is ensured by the application. Recovery from sudden blunders must be considered and the application ought to guarantee that clients won't lose their information. Applications ought to give the client the most recent security includes with a specific end goal to feel ensured. Besides some type of notice would be helpful on the off chance that a security update is available.

I. Security should not reduce performance: It is said that if we increase security, usability decreases and if usability increases security decreases. So, enhance security features but also keep performance in mind by using efficient algorithms.

7. ASSESSMENT OF EXISTING APPLICATIONS

On the basis of HCI-S guidelines applications are accessed. Applications are evaluated and compared. The applications are Norton Antivirus, McAfee Virus Scan, Agnitum's Outpost Firewall, Opera, Mozilla Firefox web-browser, and Microsoft Word. Each application was verified against 10 guidelines. The grading technique applied for all the applications were from 0 to 5, as recorded in Table 1.

TABLE 1. GRADING TECHNIQUE

Grade	Reason
0	Application diverges completely from guideline.
1	Application significantly diverges from guideline.
2	Application has paid attention to guideline but still have major problems.
3	Application has paid attention to guideline but still have minor problems.
4	Application follows guideline in some sections.
5	Application completely follows guideline in all possible sections.

A summary of score for each application achieved from each of the 10 guidelines is shown below in Table 2.

	Firefox	Outpost	Mc Afee	Norton
Visible system state and security functions	2	3	4	2
Security should be easily used	4	3	3	4
Suitable for advanced as well as first time users	5	2	2	4
Avoid technical vocabulary or advanced terms.	2	0	4	2
Handle errors appropriately	3	2	3	2
Allow customization without risk to be trapped	2	2	0	2
Easy to setup security settings	2	5	5	2
Suitable security help and documentation	0	1	1	5
Make the user feel protected	3	4	4	3
Security should not reduce performance	3	4	1	3
TOTAL (/50)	**26**	**26**	**27**	**29**

Table 2. Summary of Applications

VIII. APPLYING THE GUIDELINES

Modification occurred in order to follow the HCI-S guidelines to many websites. The software tool Mozilla Firefox obtained comparatively low score because it did not conform to most of the HCI-S guidelines. Privacy option was present in separate tab but security option was inside advance tab which was difficult to find for new users. Therefore, grouping the security settings in an advanced tab may result in a number of users never accessing them. So in order to improve usability of the system a separate tab was introduced for security.[5]

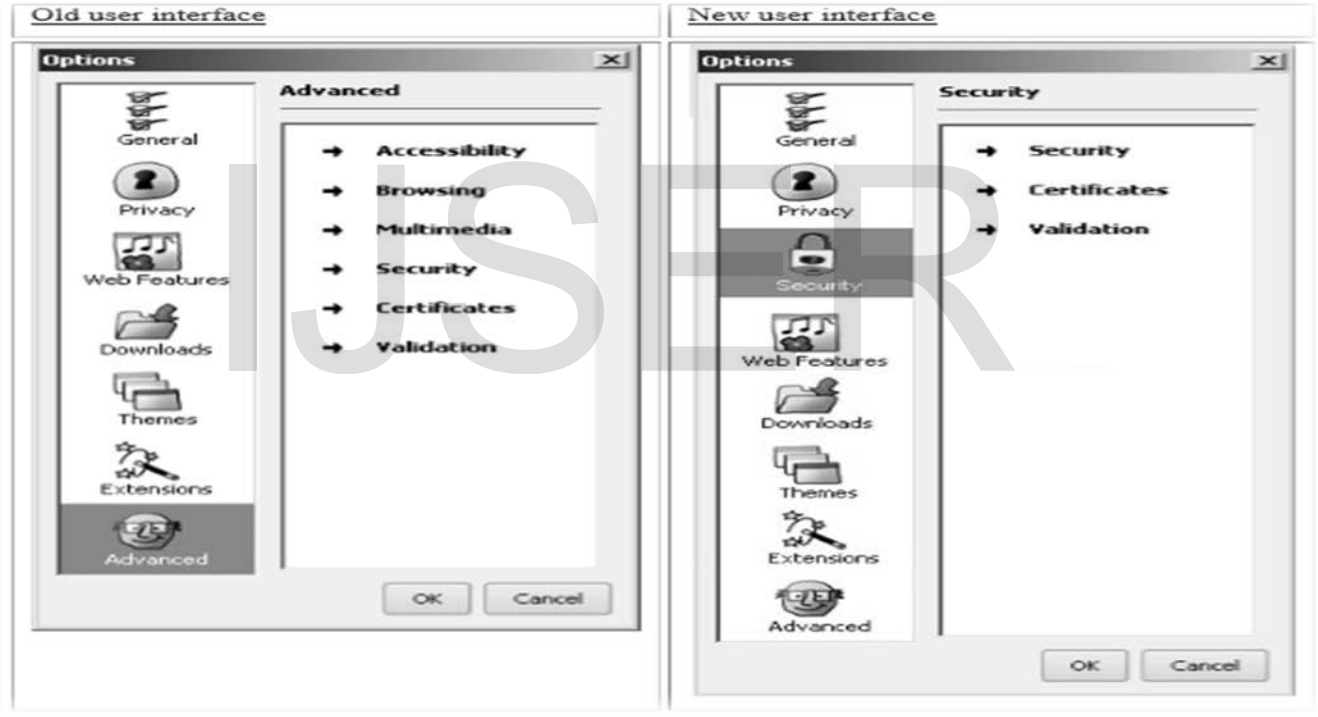

Figure 2. A new options tab

CONCLUSION

Personalized systems need to take user privacy fears into explanation. Prominent issue in systems is security violation and concerns. User hesitate to provide their personal information over internet. This problem can only be overcome by knowing the user and system. HCI deals with the interaction between the human and system. In this paper we have discussed the reason for not providing personal information to systems, the element effecting end-user and examined how these element impact users. By implementing security through human computer interaction end users now trust systems and will provide their information without hesitation. Universally, human-computer interaction lead to high level of proficiency and reliability.

REFERENCES:

[1] D.Katsabas, S.M.Furnell and A.D.Phippen. "IT Security: A Human Computer Interaction Perspective." Network Research Group, University of Plymouth, Plymouth, United Kingdom.
[2] M.M. ELOFF, J.H.P. ELOFF. "HUMAN COMPUTER INTERACTION: AN INFORMATION SECURITY PERSPECTIVES." RAU Standard Bank Academy for Information Technology Rand Afrikaans University, Johannesburg, South Africa.
[3] Giovanni Iachello and Jason Hong. "End-User Privacy in Human–Computer Interaction." Foundations and TrendsR in Human–Computer Interaction Vol. 1, No. 1 (2007) 1–137.
[4] Hussain Mohammad Abu Dalbouh. "Implementing End-User Privacy through Human Computer Interaction for Improving Quality of Personalized Web." Computer and Information Science; Vol. 9, No. 1; 2016.
[5] West, Ryan. "HCI and security." INTERACTIONS-NEW YORK-13.3 (2006): 18.
[6] Patrick, Andrew S., A. Chris Long, and Scott Flinn. "HCI and security systems." CHI'03 Extended Abstracts on Human Factors in Computing Systems. ACM, 2003.